

Wisconsin's data breach notification law

Section 134.98 of the Wisconsin Statutes requires most businesses to notify individuals if an unauthorized person has acquired their personal information. The business must be operating in Wisconsin and maintaining personal information about individuals who reside in Wisconsin. This law also applies to Wisconsin state government agencies, cities, towns, villages, and counties.

What personal information is covered

The law defines personal information to mean an individual's last name and first name or first initial in combination with and linked to any of the following elements, if the element is not publicly available information, and is not encrypted, redacted or altered in a manner that renders the element unreadable:

- Social security number.
- Driver's license number or state identification number.
- Financial account number including a credit or debit card account number or any security code, access code or password that would permit access to the individual's financial account.
- DNA profile.
- Any unique biometric data including fingerprint, voiceprint, retina or iris image, or any other unique physical representation.

Who is required to give notice

Among those required to give notice are:

- Businesses that conduct business in the state and maintain personal information in the ordinary course of business.
- Businesses that license personal information in the state.
- Businesses that maintain a depository account for Wisconsin residents.
- Businesses that lend money to Wisconsin residents.
- The state and any office, department, independent agency, authority, institution, association, society or other body in state government created or authorized by Wisconsin law including the courts and the legislature.
- A city, village, town or county.

Certain financial institutions that are subject to and in compliance with the privacy and security requirements of federal law, as well as businesses that have contractual arrangements with such institutions and have a

policy in effect regarding security breaches, are exempt from Wisconsin's law. Similarly, certain health plans and health care providers are not covered by Wisconsin's law.

When is notice required

Generally, the law requires the business or governmental entity to notify an individual whenever personal information held by the business or governmental entity is acquired by an unauthorized person. However, no notice is required if the unauthorized acquisition does not create a material risk of identity theft or fraud, or if the information was acquired in good faith by an employee or agent and is used for a lawful purpose of the entity.

What notice is required

In general, any entity that is required to give notice of the unauthorized acquisition of personal information must provide notice of that fact to persons whose information was acquired. The notice must be given within a reasonable time, not to exceed 45 days after the entity learns of the unauthorized acquisition. The notice must be given by mail or by a method that the entity has previously used to communicate with the subject of the information. For example, if a business has communicated with a customer by email, notice may be given by email. Upon written request of the person whose information was acquired, the entity must also identify the nature of the personal information acquired.

If an entity cannot determine the mailing address of the person whose information was acquired, and if the entity has not previously communicated with that person, the entity must give notice in a manner that is reasonably calculated to provide notice. Such methods might include notice in the newspaper or on television or radio.

In cases where the personal information of more than 1,000 individuals was acquired at one time, the entity from which the information was required must also give notice to all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis. This would include the major credit reporting agencies.

A law enforcement agency may request that an entity not provide notice in order to protect an investigation or homeland security. In such cases, the entity may not provide notice until permitted by the law enforcement agency.

Two-factor authentication

Two factor authentication is an added layer of security that combines something you have, a physical token such as a card or a code, with something you know, something memorized such as a personal identification number (PIN) or password.

For more information or to file a complaint, visit our website or contact the Bureau of Consumer Protection.

Bureau of Consumer Protection
2811 Agriculture Drive
PO Box 8911
Madison WI 53708-8911

E-MAIL:
DATCPWisconsinPrivacy@Wisconsin.gov

WEBSITE: datcp.wi.gov

(800) 422-7128

(608) 224-4976

FAX: (608) 224-4677

TTY: (608) 224-5058